OLR Bill Analysis

sSB 117 (File 340, as amended by Senate "A")*

AN ACT CONCERNING BREACHES OF SECURITY INVOLVING ELECTRONIC PERSONAL INFORMATION.

SUMMARY

This bill requires a person or entity with computerized data that includes personal information to promptly retain a third party for a forensic examination after discovering unauthorized access to or use of a computer network the person owns or controls that will likely result in a massive breach of security. A "massive breach of security" is a breach or a likely breach of at least 100,000 residents' personal information (other than credit or debit card numbers) through unauthorized access to or use of a computer or computer network. The law generally already requires these people and entities to notify affected individuals and the attorney general about any security breach and offer identity theft protection to certain affected individuals. It also makes it a Connecticut Unfair Trade Practices Act (CUTPA) violation to violate these provisions.

Within 60 days of discovering a breach that likely results in a massive breach of security, the bill requires the person or entity to give the attorney general, in a way set by the attorney general, a reasonable timeline for (1) preparing the forensic report and (2) submitting it, if requested, to the attorney general. If the person or entity does not submit a requested report in a way set by the attorney general, the attorney general can have a third party conduct the examination and produce a report.

The bill delays a required forensic examination if a law enforcement agency requests a delay because the examination will impede a criminal investigation. The delay ends when the law enforcement agency issues notice that the examination will not compromise the investigation.

The bill exempts these forensic reports and other information related to investigations under the bill from disclosure under the Freedom of Information Act (FOIA). It also (1) makes violations of the bill a CUTPA violation that is enforced by the attorney general and (2) authorizes a civil penalty of up to $250,000 for failing to submit a requested forensic report to the attorney general.

The bill (1) requires a person or entity that licenses or maintains personal information to use reasonable data security and (2) cannot be construed to provide that a person or entity that reports a massive security breach has used unreasonable data security.

The bill also makes minor, technical, and conforming changes, including that when the law requires certain security breach notices to the attorney general, they be in a form and manner set by the attorney general.

*Senate Amendment "A" (1) excludes credit and debit card numbers from the types of personal data that can be part of a massive breach of security; (2) requires a person or entity to promptly, instead of immediately, retain a third party for an examination and report; (3) specifies that a person or entity can work with the third party and take steps to remediate a massive breach; (4) adds provisions on use of reasonable data security and that reporting a massive breach is not construed as using unreasonable data security; and (5) adds financial distress as a factor to consider when setting the amount of a civil penalty.

EFFECTIVE DATE: October 1, 2026

FORENSIC EXAMINATION AND REPORT

The bill requires the third party retained for a forensic examination under the bill to have experience in forensic examinations and analyzing computers or computer networks. The third party must produce a detailed forensic report that includes (1) the examination and analysis results and (2) how the unauthorized access or use occurred and its root causes, if known.

The person or entity discovering the massive breach of security must pay for the cost of the examination, analysis, and report, whether the third party is retained by the person or entity or the attorney general.

The bill specifies that it does not prohibit a person or entity who reports a massive security breach from (1) working with the third party in the investigation or report preparation or (2) taking appropriate actions to investigate and remediate the breach.

FOIA

Under existing law, information provided as part of a response to an investigation of a CUTPA violation related to a security breach is exempt from disclosure under FOIA, but the attorney general may give this information to third parties as part of the investigation. The bill extends this exemption to cover CUTPA investigations related to the bill's provisions, exempts the bill's required forensic reports from disclosure under FOIA, and allows the attorney general to make the reports available to third parties as part of a CUTPA investigation.

The bill specifies that submitting the forensic reports to the attorney general does not waive the attorney-client privilege or work product protection, if it applies to specific information in the reports.

PENALTIES

By law, failing to comply with existing law's security breach notice requirements is a CUTPA violation, enforceable by the attorney general. The bill expands this to also include violations of the bill's requirements.

In addition to CUTPA penalties, the bill authorizes a civil penalty of up to $250,000 for failure to submit a requested forensic report. The bill requires a court, presumably if reviewing the amount of the civil penalty, to consider whether the business is (1) a for profit small business with up to 500 employees, (2) an independently owned and operated business with less than 50 full-time employees or less than $5 million in gross annual sales (a micro business), (3) a nonprofit entity employing up to 500 employees or less than 50 full-time employees, or (4) under financial distress.

As with civil penalties related to violating the law's security breach notice requirements, the bill permits depositing civil penalties collected for violating the bill's provisions in the privacy protection guaranty and enforcement account. By law, this account is used to enforce certain laws about safeguarding personal information and reimburses individuals hurt by violations of these provisions.

BACKGROUND

Breach of Security

By law, a "breach of security" is unauthorized access to, or acquisition of, electronic files, media, databases or computerized data containing personal information when access to that information has not been secured by encryption or alternate means rendering it unreadable or unusable.

Personal Information

By law, "personal information" includes a person's first name or first initial and last name combined with certain information such as a social security, taxpayer identification, driver's license, credit or debit card number; medical or biometric information; geolocation data; or user name or email address combined with a password or security question and answer. It does not include information that is lawfully available to the public from government or widely distributed media.

CUTPA

By law, CUTPA prohibits businesses from engaging in unfair and deceptive acts or practices. It allows the Department of Consumer Protection commissioner, under specified procedures, to issue regulations defining an unfair trade practice, investigate complaints, issue cease and desist orders, order restitution in cases involving less than $10,000, impose civil penalties of up to $5,000**,** enter into consent agreements, ask the attorney general to seek injunctive relief, and accept voluntary statements of compliance. It also allows individuals to sue. Courts may issue restraining orders; award actual and punitive damages, costs, and reasonable attorney's fees; and impose civil penalties of up to $5,000 for willful violations and up to $25,000 for a

restraining order violation.

COMMITTEE ACTION

General Law Committee

Joint Favorable Substitute
Yea 21 Nay 0 (03/16/2026)

Judiciary Committee

Joint Favorable
Yea 40 Nay 0 (04/10/2026)